



9.8 1200

Attorney Docket
No. B-68149 (014354/0004)



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box **PATENT APPLICATION**
Assistant Commissioner
for Patents
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is the patent application of:

Inventors: Rodriguez, et al.

For: SYSTEM AND APPARATUS FOR CREDIT TRANSACTION DATA
TRANSMISSION

Enclosed are:

<u>1</u> pages of abstract	<u>X</u>	Combined Declaration/Power of Attorney
<u>25</u> pages of specification	<u>—</u>	Small Entity Statement – Small Business Concern
<u>6</u> pages of claims	<u>X</u>	Assignment w/Recordation Page
<u>5</u> pages of informal drawings	<u>X</u>	Other: Check & Post Card Receipt

X **Post Office Express Mail Certificate No. NB 437 682 51X**

The filing fee has been calculated as shown below:

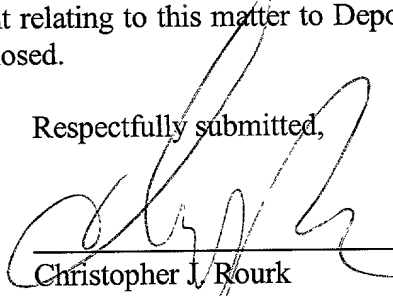
For:	No. Filed	No. Extra	Rate	<u>Large Entity</u> <u>Fee</u>
Basic Fee				\$ 690.00
Total Claims	21 - 20	-1-	x \$ 18.	18.00
Indep. Claims	4 - 3 =	-1-	x \$ 36.	36.00
Multiple dependent claims	-0-		+ \$260.	0.00
			TOTAL	\$ 744.00

Our check in the amount of \$744.00 in payment of the filing fee is enclosed.

The Commissioner of Patents and Trademarks is hereby authorized to charge any fee deficiency or to credit any fee overpayment relating to this matter to Deposit Account No. 01-0657. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

Date: 9/7/20


Christopher J. Rourke
Attorney for Applicant
Registration No. 39, 348

AKIN, GUMP, STRAUSS, HAUER & FELD, L.L.P.
P.O. Box 688
Dallas, TX 75313-0688
Phone: 214/969-2800

5 IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

SPECIFICATION
accompanying

10

Application for Grant of U.S. Letters Patent

15

TITLE: SYSTEM AND APPARATUS FOR CREDIT TRANSACTION DATA
TRANSMISSION

20

FIELD OF THE INVENTION

The present invention pertains to the field of payment
data processing. More specifically, the invention relates
25 to a system and apparatus for transmitting credit
transaction data that allows the credit transaction data to
be transmitted over a communications medium.

BACKGROUND

Electronic payment systems are used to receive credit and other electronic payment data and to transfer an authorization request that includes the credit transaction data to an authorization system. The authorization system then verifies whether the form and amount of payment is valid, and an authorization code is generated for transmission to the point of sale that authorizes the transaction, denies the transaction, notifies the operator or potential criminal activity, or provides other suitable data. In this manner, fraudulent activities using electronic payment on credit cards can be minimized.

Current authorization systems utilize the public switched telephone network for authorization. The point of sale terminal must establish a telephone connection with the authorization host, such as by a dial-up connection or by using a leased line with a permanent connection. Such connections through the public switched telephone network or through leased lines are expensive to maintain, and may experience communications failure.

A second method by which point of sale terminals may be connected with an authorization host is through the Internet or other online communications media through a virtual private network device. The virtual private network device encodes data received from the point of sale terminals and then decodes the data at the authorization host. Such virtual private network devices cannot be remotely programmed, are typically made from hardware or otherwise not designed to be updated with new programming, and do not provide communications from the authorization system to the point of sale system, such as to determine the status of

point of sale system. In addition, such virtual private network devices are not compatible with standard network architecture and must be installed outside of the network firewall. In addition, failure of the virtual private
5 network device can result in communications failure.

Thus, while credit transaction authorization is presently performed over communications media, such authorization either is at high cost, in that it requires connections to be made over the public switched telephone
10 network, or in that it requires expensive virtual private network devices that are not compatible with existing networks and which must be changed out in the event of a security violation. In addition, the credit transaction data that can be transmitted is limited and cannot be readily
15 modified in response to standards changes, technological changes, or for other reasons.

SUMMARY OF THE INVENTION

In accordance with the present invention, a system and apparatus for transmitting credit transaction data are provided that overcome known problems with transmitting credit transaction data.

In particular, a system and apparatus for transmitting credit transaction data are provided that allow credit transaction data to be transmitted over the Internet or other communications media, by allowing the encryption procedures used on the credit transaction data to be readily updated so as to protect system security.

In accordance with an exemplary embodiment of the present invention, a system for transmitting credit transaction data, such as credit card data, account number data, vendor number data, user identification data, password data, PIN number data, an authorization request, or other suitable data, is provided. The system includes a remote hub system that is connected to a communications medium, such as the Internet. The remote hub system receives credit transaction data, such as an authorization request, a credit card number, and a transaction amount, from one or more point of sale systems, such as credit card authorization terminals. The remote hub system then encrypts the credit transaction data, and transmits the encrypted credit transaction data over the Internet to a gateway system. The gateway system decrypts the encrypted credit transaction data and transmits the credit transaction data to an authorization system.

The present invention provides many important technical advantages. One important technical advantage of the present invention is a system and apparatus for transmitting credit

transaction data that allows the encryption procedure to be readily modified. The present invention thus allows the Internet or other unsecured communications media to be used to transmit credit transaction data by allowing encryption
5 procedures that are used to maintain the security of the credit transaction data to be readily updated.

Those skilled in the art will further appreciate the advantages and superior features of the invention together with other important aspects thereof on reading the detailed
10 description that follows in conjunction with the drawings.

002000-5789990

FIGURE 1 is a diagram of a system for providing online credit transaction data transmission in accordance with an exemplary embodiment of the present invention;

5

10

15

FIGURE 5 is a diagram of a system for providing remote hub access to a gateway system in accordance with an exemplary embodiment of the present invention;

20

FIGURE 7 is a diagram of a method for processing credit transaction data in accordance with an exemplary embodiment of the present invention; and

25

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the description which follows, like parts are marked throughout the specification and drawings with the same reference numerals, respectively. The drawing figures may not be to scale and certain components can be shown in generalized or schematic form and identified by commercial designations in the interest of clarity and conciseness.

FIGURE 1 is a diagram of a system 100 for providing online credit transaction data transmission in accordance with an exemplary embodiment of the present invention. System 100 allows credit to be transferred over a public communications medium, such as the Internet, and allows the credit transaction data to be encrypted in a manner that allows the encryption mechanism to be modified or updated as needed.

System 100 includes remote hub system 102. Remote hub system 102 can be implemented in hardware, software, or a suitable combination of hardware, and can be one or more software systems operating on a Single Board Computer ("SBC") manufactured by EMAC, Inc. of Carbondale, Illinois, an Ericsson eBox Model 101, or other suitable Open Services Gateway Initiative (OSGI) compliant appliances. As used herein, a software system can include one or more lines of code, objects, agents, subroutines, one or more lines of code operating in two or more different software programs, two or more separate software programs, or other suitable software architectures. In one exemplary embodiment, a software system can include one or more lines of code or other suitable software structures operating in a general purpose competing program, such as an operating system, and one or more lines of code or other suitable software

structures operating in a specific purpose software application.

Remote hub system 102 receives credit transaction data from point of sale system 104 in accordance with a
5 predetermined data transmission protocol, such as the ISO 8583 protocol, the VISA-K protocol, or other suitable protocols. The credit transaction data can also include Electronic Data Interchange (EDI) format data, credit card data, account number data, vendor number data, user
10 identification data, password data, PIN number data, an authorization request, or other suitable data. Remote hub system 102 then encrypts the credit transaction data, and transmits the credit transaction data as an authorization request over a communications medium 112 to gateway system
15 106. Authorization data is then received at remote hub system 102 from an authorization system through gateway system 106, and is transmitted to the point of sale system 104 by remote hub system 102.

Remote hub system 102 can also receive data from
20 gateway system 106 through communications medium 112, such as data that can be used to control the operation of remote hub system 102, requests for status, or other suitable data. Remote hub system 102 can use a data format that is amenable for transmission through local area network or wide area
25 network firewalls, such as HyperText Transfer Protocol ("HTTP") format data, eXtensible Markup Language (XML), or other format data, such that remote hub system 102 can be installed at any point within a network without consideration for the location of that position in regards
30 to the network firewall.

Point of sale system 104 is coupled to remote hub

002000-5739560
15
10
system 102, and can be implemented in hardware, software, or a suitable combination of hardware and software, and can be one or more software systems operating on a point of sale terminal or device. As used herein, the term "couple" and its cognate terms, such as "couples" and "coupled," can include a physical connection (such as a copper conductor), a virtual connection (such as through randomly assigned memory locations of a data memory device), a logical connection (such as through logical devices of a semiconducting circuit), a combination of such connections, or other suitable connections. In one exemplary embodiment, systems and components are coupled to other systems and components through intervening systems and components, such as through an operating system of a processor platform.

15 Point of sale system 104 can receive credit transaction data from a magnetic stripe of a credit card, data entered by a user through a terminal, or other suitable forms of credit or electronic payment data, and can transmit the data to remote hub system 102 in a suitable format. Point of
20 sale system 104 also receives authorization data from an authorization system through remote hub system 102, and uses the authorization data to determine whether to accept or reject a credit or electronic payment transaction.

25 Gateway system 106 can be implemented in hardware, software, or a suitable combination of software and hardware, and can be one or more software systems operating on a general-purpose server platform. Gateway system 106 receives encrypted credit transaction data from remote hub system 102 over communications medium 112 and converts the
30 encrypted credit transaction data into credit transaction data in a format suitable for transmission to authorization

system 108. Gateway system 106 can also transmit data to remote hub system 102, such as data requesting the status of remote hub system 102 or point of sale system 104, protocol modules for updating the credit transaction data format protocols used by remote hub system 102, encryption modules for updating the encryption process used by remote hub system 102, and other suitable data. Gateway system 106 can also interface with multiple authorization systems 108, such that data received from remote hub system 102 can be routed to a suitable authorization system.

Authorization system 108 can be implemented in hardware, software, or a suitable combination of hardware and software, and can be one or more software systems operating on a general-purpose server platform. Authorization system 108 receives credit transaction data from gateway system 106 and performs an authorization analysis on the credit transaction data. In one exemplary embodiment, authorization system 108 checks a credit card number against a list of reported stolen credit card numbers, a list of credit card numbers that are over their credit limit, and a list of credit card numbers for which monitoring of the credit card has been initiated. Authorization system 108 then transmits suitable data to gateway system 106, such as a code authorizing or denying the use of the credit card for the credit transaction.

Transaction system 110 can be implemented in hardware, software, or a suitable combination of hardware and software, and can be one or more software systems operating on a general-purpose server platform. Transaction system 110 receives credit transaction data from gateway system 106 and performs credit transaction processing. In one

Communications medium 112 is coupled to remote hub system 102 and gateway system 106 and allows communications to flow between remote hub system 102 and gateway system 106. In one exemplary embodiment, communications medium 112 is the Internet, but can also or alternatively include a local area network, a wide area network, a wireless network, the public switched telephone network, a suitable combination of such media, or other suitable communications media. In another exemplary embodiment, communications medium 112 is the Internet and also includes a connection through the public switched telephone network that can be used in the event that the Internet is unavailable.

System 100 further allows remote hub system 102 to interface with point-of-sale devices and other devices so as to recognize the device and set configuration parameters to allow the point-of-sale devices and other devices to communicate with the transaction systems, authorization

systems, and other systems, so as to allow point of sale devices and other devices that were not previously able to communicate over the Internet, to receive and transmit data to these systems. Any non-HTTP-based communications protocol used by such devices, such as email, socket connections, File Transfer Protocol (FTP), any TCP/IP protocol that isn't inherently securable, and other protocols can be accomodated.

FIGURE 2 is a diagram of system 200 for transmitting credit transaction data from multiple point of sale terminals to multiple authorization systems or transaction systems in accordance with an exemplary embodiment of the present invention. System 200 allows multiple authorization systems and transaction systems to connect to one or more remote hub systems through a public online communications medium or other suitable communications media. In the exemplary embodiment shown in FIGURE 2, two authorization systems only are shown, but system 200 can also be used with three or more authorization systems, one or more transaction systems, and a suitable combination of authorization systems and transaction systems.

System 200 includes remote hub systems 102a and 102b, which are coupled to point of sale systems 104a and 104b, respectively. Gateway system 106 of system 200 is coupled to authorization systems 108a and 108b. In the exemplary embodiment shown in FIGURE 2, point of sale system 104a can interface with authorization system 108a through remote hub system 102a and gateway system 106. Likewise, point of sale system 104b can interface with authorization system 108b through remote hub system 102b. Gateway system 106 can receive the encrypted credit transaction data from remote hub

system 102a and remote hub system 102b, and can decrypt the data and determine whether the encrypted data should be transmitted to authorization system 108a or authorization system 108b. In this manner, a single gateway system can be used to connect to two or more authorization systems for use by multiple remote hub systems and point of sale systems.

FIGURE 3 is a diagram of a system 300 for transmitting credit transaction data over a communications medium in accordance with an exemplary embodiment of the present invention. System 300 allows data from two or more point of sale systems to be transmitted to one or more authorization systems or transaction systems through a single remote hub system. In the exemplary embodiment shown in FIGURE 3, an authorization system only is shown, but system 300 can also be used with two or more authorization systems, one or more transaction systems, and a suitable combination of authorization systems and transaction systems.

System 300 includes remote hub system 102, which is coupled to point of sale systems 104a, 104b and 104c through communications medium 302. Communications medium 302 can be a local area network, a wide area network, individual hard-wired connections to each point of sale system, a wireless network, or other suitable communications media. Remote hub system 102 can transmit and receive data from each of point of sale systems 104a, 104b, and 104c, such as through use of an Ethernet communications protocol, a token ring communications protocol, direct communications to each terminal, or other suitable protocols.

Remote hub system 102 can then transmit the data received from point of sale systems 104a, 104b, 104c to gateway system 106 for subsequent transmission to

authorization system 108. Likewise, multiple authorization systems can be connected to gateway system 106, such that point of sale system 104a can transmit credit transaction data to a first authorization system, point of sale system
5 104b can transmit credit transaction data to a second authorization system, and other suitable transmissions can be made. In this manner, a single remote hub system can couple a plurality of point of sale systems to one or more authorization systems through a single communications medium
10 112.

Likewise, remote hub system 102 can receive authorization data from one or more authorization systems 108 through one or more gateway systems 106, and can route the authorization data to the corresponding point of sale system
15 104a, 104b, or 104c for which the authorization data has been generated. Remote hub system 102 includes routing functionality that allows the credit transaction data received from a point of sale terminal to be matched with the corresponding authorization data received from an
20 authorization system 108. In one exemplary embodiment, remote hub system 102 maps address data to each credit transaction data message that identifies the point of sale systems 104a, 104b, or 104c that the credit transaction data was received from. This address data map is then used to
25 route the authorization data received from the authorization system 108 to the correct point of sale system 104a, 104b, or 104c. Other suitable procedures can also be used.

FIGURE 4 is a diagram of a system 400 for transmitting credit transaction data in accordance with an exemplary
30 embodiment of the present invention. System 400 allows two or more gateway systems to transmit credit transaction data

from a point of sale system to an authorization system, and to transmit the corresponding authorization data to the point of sale system. In the exemplary embodiment shown in FIGURE 4, an authorization system only is shown, but system 400 can also be used with two or more authorization systems, one or more transaction systems, and a suitable combination of authorization systems and transaction systems.

System 400 includes gateway systems 106a and 106b which are each coupled to communications medium 112. Likewise, gateway systems 106a and 106b can be coupled to each other through a communications medium 402, which can be the public switched telephone network, a leased line, or other forms of communications. Gateway systems 106a and 106b thus exchange periodic updates and can function as redundant gateway systems for access to authorization system 108.

In operation, system 400 is used to transmit credit transaction data from point of sale system 104 to remote hub system 102 and then to authorization system 108 through either or both of gateway systems 106a and gateway system 106b. Data transmitted from remote hub system 102 over communications medium 112 can be received at either or both of gateway system 106a and 106b. Gateway system 106b can be disabled while gateway system 106a is in operation, or can also be configured to receive information and transmit information redundantly to authorization system 108. In this manner, if either of gateway systems 106a or 106b fail to operate, fail to receive the credit transaction data, or otherwise become unavailable, the credit transaction data is still transferred to authorization system 108 for authorization.

FIGURE 5 is a diagram of a system 500 for providing

remote hub access to a gateway system in accordance with an exemplary embodiment of the present invention. System 500 includes remote hub system 102, encryption system 502, remote management interface 504, dynamic protocol translator 506, 5 device router 508, and telephone backup system 510, each of which can be implemented in hardware, software, or a suitable combination of hardware and software, and which can be one or more software systems operating on a Java virtual machine, such as a Single Board Computer ("SBC") manufactured by 10 EMAC, Inc. of Carbondale, Illinois.

Encryption system 502 receives credit transaction data from a point of sale system and encrypts the credit transaction data for transmission over a suitable communications medium, such as the Internet. Encryption 15 system 502 can receive credit transaction data in a first legacy protocol format from the point of sale system, and can extract the credit transaction data for transmission to a gateway system 106. Encryption system 502 then uses an encryption algorithm or other suitable encryption procedures 20 to encrypt the data in a manner that prevents the data from being intercepted by unauthorized third parties. The encrypted data is then transmitted over the communications medium to the gateway system. Encryption system 502 can also receive an encryption module and update the encryption 25 procedure used to encrypt the credit transaction data.

Remote management interface 504 can also receive data messages that have been transmitted from gateway system 106 to system 200 over a suitable communications medium. This data can either be encrypted for decryption by encryption 30 system 502, or can be transmitted in an unencrypted form. Remote management interface 504 then removes header data,

format data, and other data from the data message and performs predetermined functions based upon the content of the data message. In one exemplary embodiment, remote management interface 504 can execute code stored within the data message, such as code that installs a dynamic protocol translator module in dynamic protocol translator 506, code that installs an encryption module in encryption system 502, or suitable code.

Dynamic protocol translator 506 receives credit transaction data from a point of sale system 104 based upon one or more standard protocols for the point of sale systems. In one exemplary embodiment, dynamic protocol translator 506 translates ISO 8583 or VISA-K protocol data into a data format suitable for encryption by encryption system 502. Dynamic protocol translator 506 can also receive a protocol module and update the protocol by which it receives the credit transaction data.

Device router 508 can receive and transmit data messages from one or more point of sale systems. Device router 508 is operable to receive credit transaction data from one or more point of sale systems and to transfer the data to dynamic protocol translator 506 or encryption system 502 for subsequent transmission to an authorization server. Likewise, device router 508 can also receive data for one or more point of sale systems 104 from other or dynamic protocol translator 506 or encryption system 502, and can route the encrypted data to the appropriate point of sale system.

Telephone backup system 510 can establish a connection with the gateway system over the public switched telephone network in the event that system 500 is otherwise unable to transmit and receive data messages from the gateway system

over a preferred communications medium, such as the Internet. In one exemplary embodiment, telephone backup system 510 establishes a dial-up connection or uses a leased telephone line when no response is received to an authorization request
5 after several attempts over the preferred communications medium.

In operation, system 500 is used to control the operation of an apparatus for encrypting data received from a credit entry device or point of sale system, where credit
10 transaction data is transmitted over a communications medium such as the Internet, such as in the form of an authorization request to a gateway system to an authorization system. System 500 also allows encrypted or unencrypted data messages to be received from the gateway system over the
15 communications medium and to be handled appropriately, such as by updating encryption system 502 with an encryption module, updating dynamic protocol translator 506 with a protocol module, or by other suitable procedures.

System 500 allows credit transaction data to be received
20 from one or more point of sale systems. The credit transaction data is then processed by dynamic protocol translator 506 to extract the credit transaction data. The credit transaction data is then encrypted by an encryption system 502 and is then transmitted to a gateway system.
25 Likewise, system 500 allows data messages to be received from a gateway system 106 by a remote management interface 504, such as status requests, encryption modules, protocol modules, or other suitable data.

FIGURE 6 is a diagram of system 600 for performing
30 gateway system functions in accordance with an exemplary embodiment of the present invention. System 600 includes

gateway system 106, translator 602, authorization host
interface 604, hub manager 606, gateway interface 608,
telephone backup system 610, and transaction host interface
612, each of which can be implemented in hardware, software,
5 or a suitable combination of hardware and software, of which
can be one or more software systems operating on a general
purpose server platform.

Translator 602 receives encrypted data messages that
include credit transaction data, and decrypts the encrypted
10 data. Translator 602 can also receive encryption modules,
such that the encryption system can be updated as required to
maintain system security. Translator 602 can receive
authorization data from an authorization system, and can
encrypt the authorization data for subsequent transmission to
15 the remote hub system.

Authorization host interface 604 receives credit
transaction data from translator 602 and transmits the credit
transaction data to an authorization system. If multiple
authorization systems are used, authorization host interface
20 604 can also determine the appropriate authorization host to
transmit the credit transaction data to, such as by using
data from a credit card type identifier field, an
authorization host identifier field, or other suitable
procedures. Authorization host interface 604 can also
25 convert the credit transaction data into a format for use by
the authorization system. The authorization response from
the authorization host can also be received by authorization
host interface 604, and can be transmitted to translator 602,
directly to the remote hub system, or to other suitable
30 systems or components.

Hub manager 606 transmits status requests, encryption

module updates, protocol module updates, or other suitable data to remote hub systems, and can analyze status data received in response to the status request from the remote hub systems. In one exemplary embodiment, hub manager 606
5 periodically transmits status requests and encryption modules to remote hub systems, in order to maintain system reliability and system security. Hub manager 606 can transmit status requests and encryption modules in response to operator requests or as otherwise required.

10 Gateway interface 608 allows system 600 to interface with other gateway systems, such as to allow data about the status of remote hub systems, encryption systems or other data to be coordinated or synchronized between systems 600. In one exemplary embodiment, gateway interface 608 is used to
15 coordinate the encryption module updates and status requests such that conflicting encryption module updates are not made. Gateway interface 608 also allows credit transaction data received at a first gateway to be transmitted to a second gateway in the event the public online communications medium
20 becomes disabled or interrupted.

Telephone backup system 610 can establish a connection with the remote hub systems over the public switched telephone network in the event that system 600 is otherwise unable to transmit and receive data messages from the remote
25 hub systems over a preferred communications medium, such as the Internet. In one exemplary embodiment, telephone backup system 610 establishes a dial-up connection or uses a leased telephone line when no response is received to a message after several attempts over the preferred communications
30 medium.

Transaction host interface 612 receives credit

transaction data from translator 602 and transmits the credit transaction data to a transaction system. If multiple transaction systems are used, transaction host interface 612 can also determine the appropriate transaction host to transmit the credit transaction data to, such as by using data from a credit card type identifier field, a transaction host identifier field, or other suitable procedures. Transaction host interface 612 can also convert the credit transaction data into a format for use by the transaction system. Any response from the transaction host can also be received by transaction host interface 612, and can be transmitted to translator 602, directly to the remote hub system, or to other suitable systems or components.

In operation, system 600 allows encrypted credit transaction data to be received and translated for use by authorization systems. System 600 also allows remote hub systems and point of sale systems to be monitored for problems, and allows protocol updates to be transmitted for use by remote hub systems.

FIGURE 7 is a diagram of a method 700 for processing credit transaction data in accordance with an exemplary embodiment of the present invention. Method 700 can be used in conjunction with a remote hub system or other suitable systems.

Method 700 begins at 702 where credit transaction data is received. The credit transaction data can include a credit card number, amount, and other suitable credit transaction data, and can be received in accordance with the ISO 8583 protocol, the VISA-K protocol, or other suitable protocols. If the credit transaction data is received from one of two or more point of sale systems or other devices,

then the credit transaction data can be mapped to allow authorization data that is sent in response to an authorization request to be matched with the corresponding point of sale system. The method then proceeds to 704.

5 At 704, the credit transaction data is assembled into an authorization request and encrypted, such as by using an updateable encryption module of an encryption system. The method then proceeds to 706, where the encrypted authorization request and credit transaction data is
10 transmitted over a suitable communications medium, such as the Internet, a local area network, a wide area network, a wireless network, or other suitable communications media. The encrypted authorization request and credit transaction data can be transmitted in packets, in HTTP format, or by
15 other suitable procedures. The method then proceeds to 708.

At 708, the encrypted authorization request and credit transaction data is received and the method proceeds to 710 where the authorization request and credit transaction data is decrypted. In one exemplary embodiment, the encrypted
20 authorization request and credit transaction data is received at a gateway system and a decryption method is used that is coordinated with the encryption method used at a remote hub system. The method then proceeds to 712.

At 712, an authorization host for the authorization
25 request and credit transaction data is determined. For example, an authorization request and credit transaction data may be received for one or more credit card issuing organizations, such as a Visa card, a MasterCard, an American Express card, or other suitable credit cards. Each of these
30 credit card issuing organizations may have its own authorization host, or a single authorization host can be

used that performs authorization services in lieu of the issuing card organization. After the authorization host is determined at 712, the method proceeds to 714 where the authorization request and the credit transaction data is
5 transmitted to the authorization host for authorization. The method then proceeds to 716.

At 716, it is determined whether authorization has been granted. If authorization has been granted, the method proceeds to 718 where credit authorization data is
10 transmitted to the point of sale system, such as by transmitting through a gateway system to a remote hub system, and then by using mapped authorization request and credit transaction data to identify the point of sale system to which the authorization data should be transmitted. If it is
15 determined at 716 that authorization has been denied, a data message is transmitted to the point of sale system that instructs the operator that the credit transaction has been denied. Likewise, additional data such as theft warning data can be transmitted.

20 An operation, method 700 allows authorization requests and credit transaction data to be transmitted over a communications medium in a manner that allows the data to be encrypted and the encryption mechanism to be changed. Method 700 allows multiple authorization systems and remote hub
25 systems to be coupled through a single gateway system.

FIGURE 8 is a diagram of a method 800 for processing remote management messages in accordance with an exemplary embodiment of the present invention. Method 800 begins at 802 where a remote management message is received, such as at
30 a remote hub system. The method then proceeds to 806 where it is determined whether a status request has been received.

0955345-000700

If a status request has been received at 804 the method proceeds to 806 where status data is obtained and transmitted. In one exemplary embodiment, the status data can include status data for a remote hub system and one or more point of sale systems coupled to the remote hub system, such as operability state data, encryption module data, protocol module data, terminal setup data, historical data such as the number of authorization requests for which a telephone backup system was used, and other suitable data. The method then proceeds to 808. Likewise, if it is determined at 804 that a status request has not been received, the method proceeds directly to 808.

At 808, it is determined whether a protocol update has been received. If no protocol update has been received, the method proceeds to 812, otherwise the method proceeds to 810 where the protocol module is stored in a suitable dynamic protocol translator system, such as one that is used to control the transmission of credit transaction data to and from a point of sale system. The method then proceeds to 812.

At 812, it is determined whether an encryption module update has been received. The encryption module update can be used to modify an encryption system so as to maintain system security. If it is determined that an encryption module update has been received at 812 the method proceeds to 814 where the encryption module update is stored in a suitable encryption system. Otherwise, the method proceeds to 813 and terminates.

In operation, method 800 allows remote hub management messages to be transmitted from a gateway system to a remote hub system to facilitate the transmission of encrypted credit

transaction data over a communications medium, such as the Internet. Method 800 allows status data to be requested from the remote hub system and any point of sale systems used in conjunction with the remote hub system, allows protocol modules to be transmitted for use by the remote hub system, allows encryption data to be transmitted so that the encryption process can be modified as required, and allows other suitable management data to be received and processed by the remote hub.

Although preferred and exemplary embodiments of a system and apparatus for credit transaction data transmission have been described in detail herein, those skilled in the art will also recognize that various substitutions and modifications can be made to the systems and methods without departing from the scope and spirit of the appended claims.

5

10

7. The system of claim 1 further comprising:

20

25

30

8. The system of claim 1 wherein the remote hub system further comprises:

5 a protocol translator receiving the credit transaction data from the one or more point of sale systems according to a transmission protocol; and

an encryption system coupled to the protocol translator, the encryption system receiving the credit transaction data from the protocol translator and encrypting
10 the credit transaction data.

002000-9789990

9. An apparatus for transmitting credit transaction data over a communications medium comprising:

a protocol translator receiving the credit transaction data from one or more point of sale systems according to a transmission protocol; and

an encryption system coupled to the protocol translator, the encryption system receiving the credit transaction data from the protocol translator and encrypting the credit transaction data.

10

10. The apparatus of claim 8 further comprising a device router coupled to the protocol translator, the device router transmitting authorization data received in response to the credit transaction data to the one or more point of sale systems in response to the credit transaction data and the authorization data.

11. The apparatus of claim 8 further comprising a management system interface coupled to the protocol translator, the management system storing a protocol module to the protocol system.

12. The apparatus of claim 8 further comprising a management system interface coupled to the encryption system, the management system storing an encryption module to the encryption system.

13. A method for transmitting credit transaction data over a communications medium comprising:

receiving credit transaction data from a point of sale device;

5 encrypting the credit transaction data;

transmitting the encrypted credit transaction data over the communications medium;

decrypting the encrypted credit transaction data;

determining which of two or more authorization systems
10 is the appropriate authorization system to provide the credit transaction data to; and

transmitting the credit transaction data to the appropriate authorization system.

15 14. The method of claim 13 wherein receiving the credit transaction data from the point of sale device comprises receiving credit transaction data from one of two or more point of sale devices.

20 15. The method of claim 13 wherein encrypting the credit transaction data comprises encrypting the credit transaction data using an encryption module received from a hub manager.

25 16. The method of claim 13 wherein transmitting the encrypted credit transaction data over the communications medium comprises transmitting the encrypted data in an HTTP format.

```
transmitting one or more control messages to a remote
hub;
```

18. The method of claim 17 wherein performing the
10 control function at the remote hub in response to the
control message comprises transmitting status data for the
remote hub.

19. The method of claim 17 wherein performing the
15 control function at the remote hub in response to the
control message comprises transmitting status data for one
or more point of sale devices connected to the remote hub.

20 20. The method of claim 17 wherein performing the
control function at the remote hub in response to the
control message comprises updating the remote hub with a
protocol module.

21. The method of claim 17 wherein performing the
25 control function at the remote hub in response to the
control message comprises updating the remote hub with an
encryption module.

ABSTRACT OF THE DISCLOSURE

5 A system for transmitting credit transaction data, such
as an authorization request, is provided. The system
includes a remote hub system that is connected to a
communications medium, such as the Internet. The remote hub
system receives credit transaction data, such as an
authorization request, a credit card number, and a
10 transaction amount, from one or more point of sale systems,
such as credit card authorization terminals. The remote hub
system then encrypts the credit transaction data, and
transmits the encrypted credit transaction data over the
Internet to a gateway system. The gateway system decrypts
15 the encrypted credit transaction data and transmits the
credit transaction data to an authorization system.

0055315-000700

FIGURE 1
014354.0004

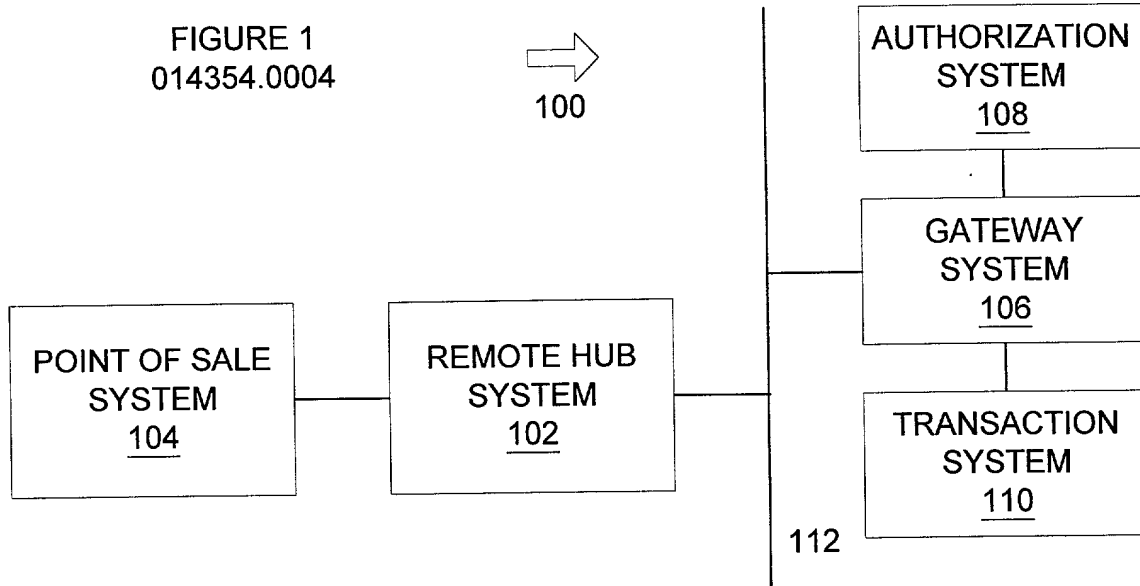
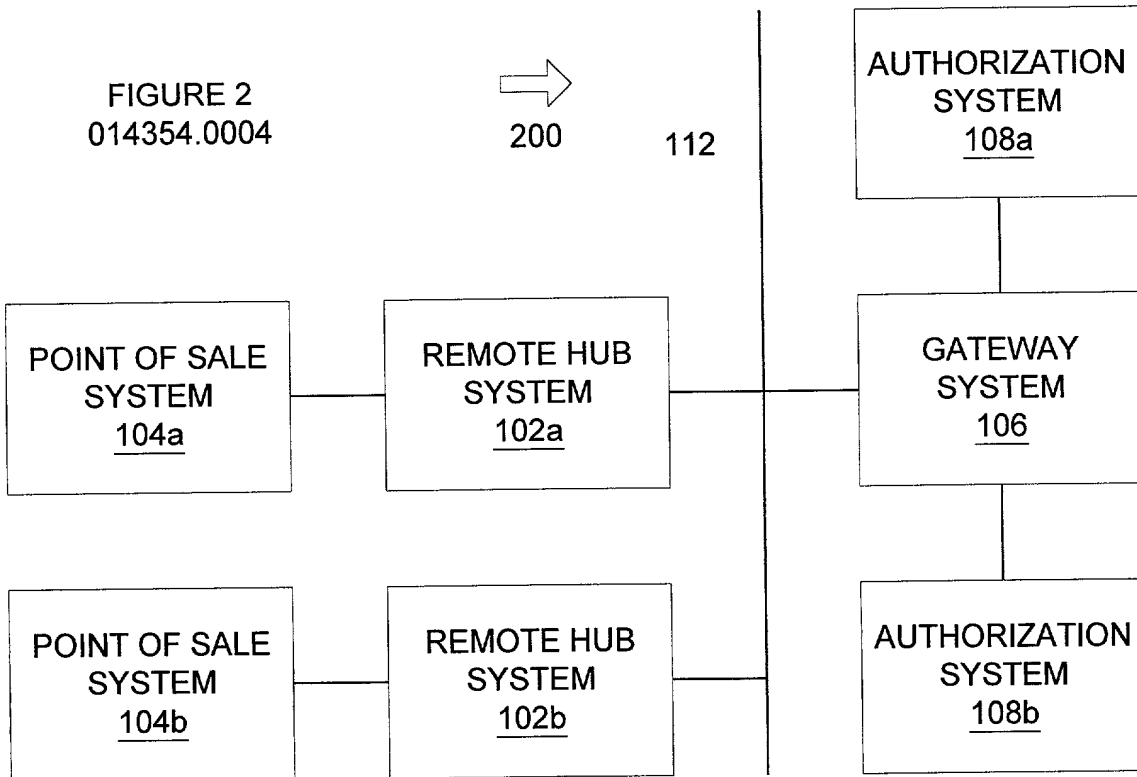
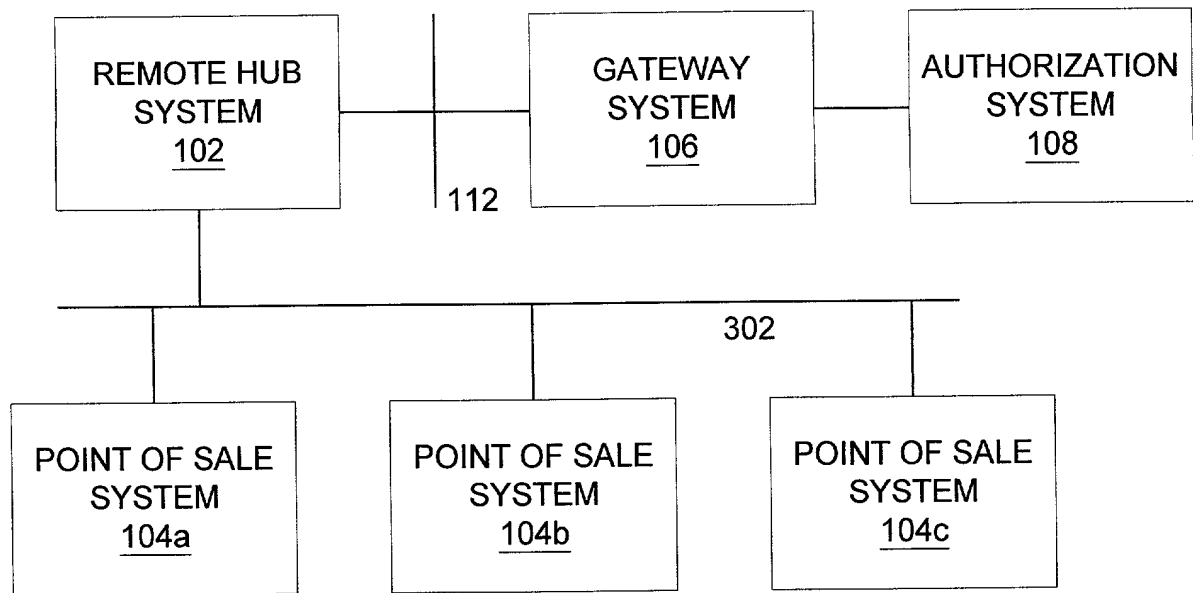


FIGURE 2
014354.0004

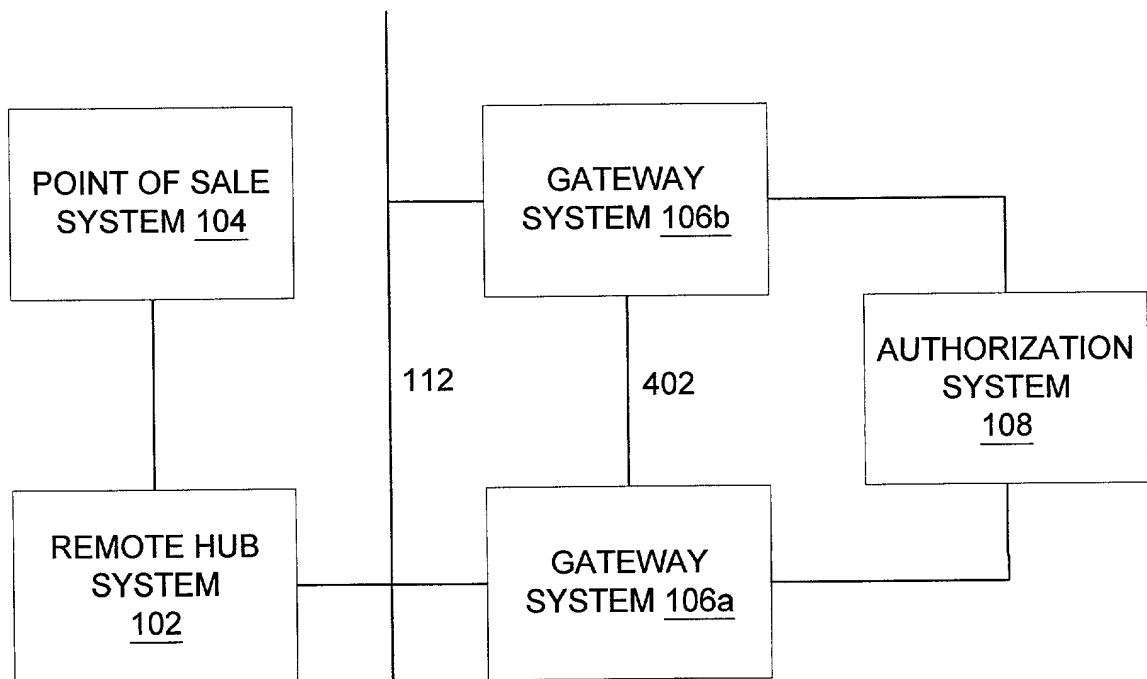


002060-9789960



300 ↑

FIGURE 3
014354.0004



400 ↑

FIGURE 4
014354.0004

002060-5789960

The diagram illustrates a network architecture with a central vertical bus. On the left side of the bus, three components are connected: a TRANSLATOR 602, a TELEPHONE BACK-UP SYSTEM 610, and a HUB MANAGER 606. On the right side of the bus, three components are connected: an AUTHORIZATION HOST INTERFACE 604, a TRANSACTION HOST INTERFACE 612, and a GATEWAY INTERFACE 608. Each component is enclosed in a rectangular box, and the bus is represented by a central vertical line with horizontal lines connecting to each component.

```
graph LR; T602[TRANSLATOR 602] --- Bus; TB610[TELEPHONE BACK-UP SYSTEM 610] --- Bus; HM606[HUB MANAGER 606] --- Bus; Bus --- AHI604[AUTHORIZATION HOST INTERFACE 604]; TH612[TRANSACTION HOST INTERFACE 612] --- Bus; GI608[GATEWAY INTERFACE 608] --- Bus;
```

FIGURE 6
014354.0004

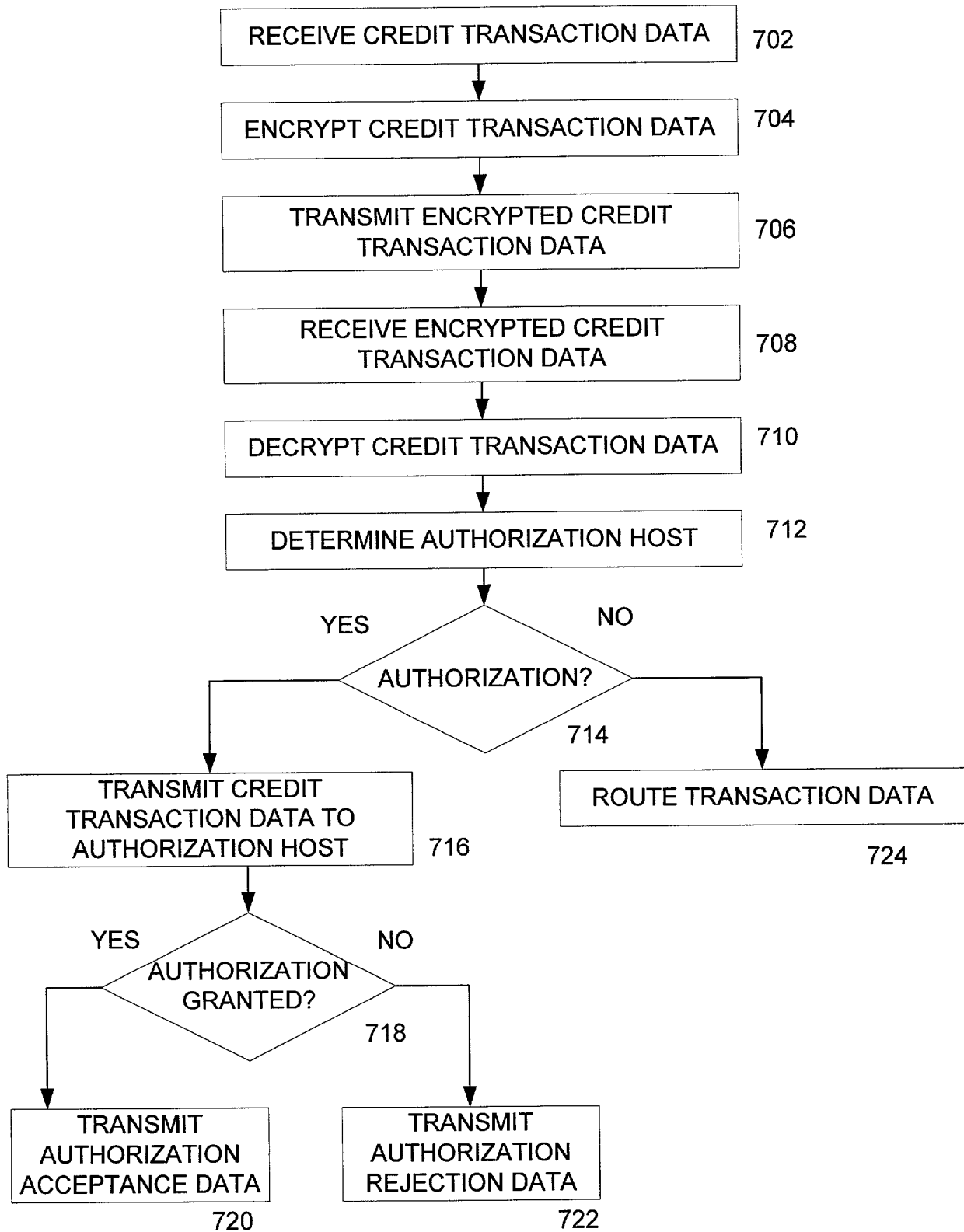


FIGURE 7
014354.0004

↑ 700

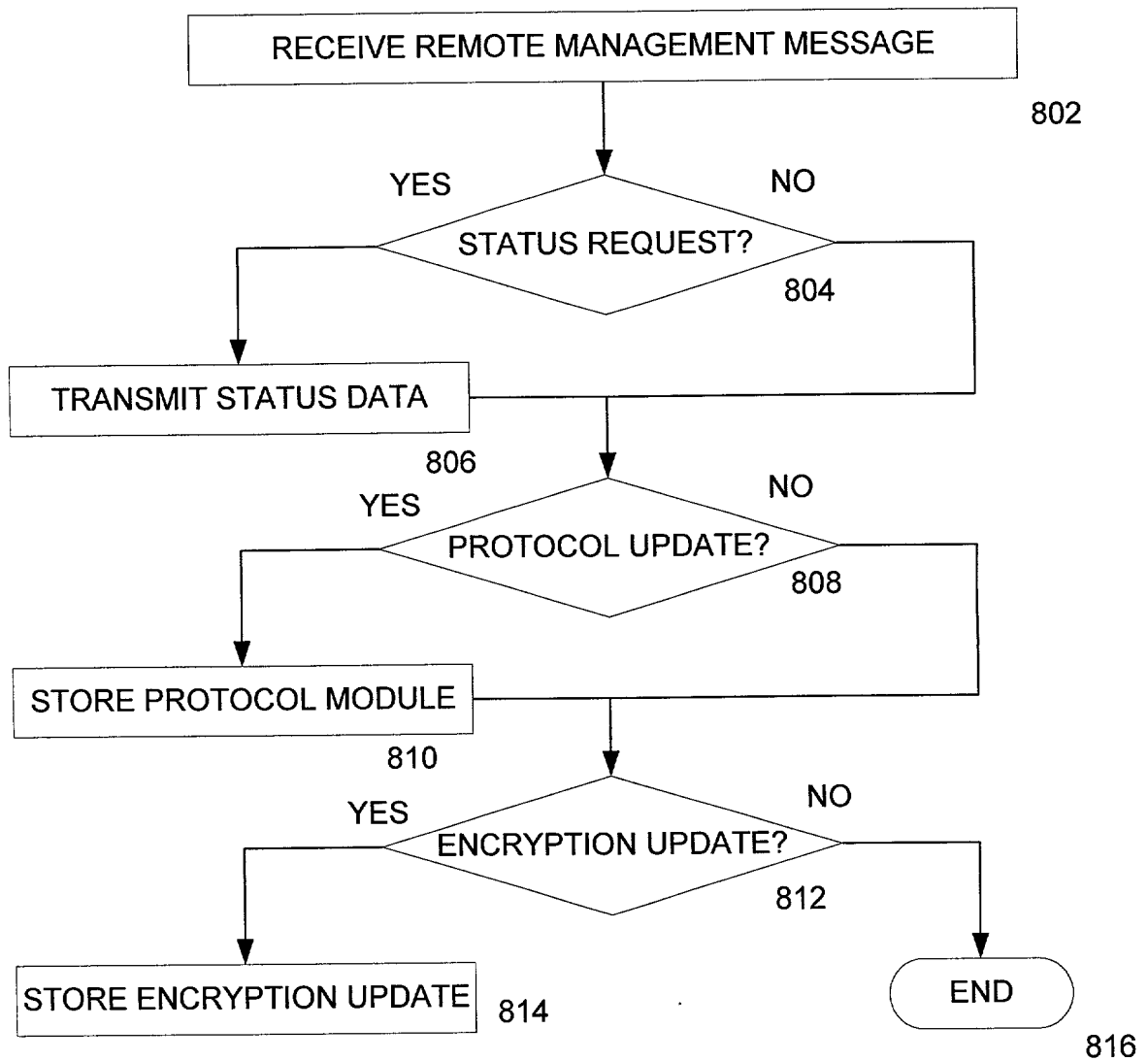


FIGURE 8
014354.0004

DECLARATION AND POWER OF ATTORNEY

We, Alan F. Rodriguez, Jr., Christopher W. Cross, Dorwin Shields, Jr., and David T. Meckenstock, joint inventors herein, hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names.

We believe that we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled

"SYSTEM AND APPARATUS FOR CREDIT DATA TRANSMISSION",

the specification of which is attached hereto.

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to in this declaration.

We acknowledge the duty to disclose to the Patent and Trademark Office all information known to us to be material to the patentability of any claim in accordance with Title 37, Code of Federal Regulations, §1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable examiner would consider it important in deciding whether to allow the application to issue as a patent.

We hereby appoint ; CHRISTOPHER J. ROURK, Registration No. 39,348, STEVEN E. ROSS, Registration No. 35,996, KENNETH R. GLASER, Registration No. 24,015; RANDALL C. BROWN, Registration No. 31,213; JOHN M. CONE, Reg. No. 30,538; MICHAEL E. MARTIN, Registration No. 24,821; PRISCILLA L. FERGUSON, Registration No. 42,531; JOHN R. EMERSON, Registration No. 44,098 and ALVIN R. WIRTHLIN, Registration No. 40,267 of the firm of AKIN, GUMP, STRAUSS, HAUER & FELD, L.L.P., our attorneys and agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith. Send all correspondence to:

Christopher J. Rourk
AKIN, GUMP, STRAUSS, HAUER & FELD, L.L.P.
P.O. Box 688
Dallas, TX 75313-0688
Phone: 214/969-4669

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these

all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this application or any patent issued thereon.

Full Name of


First Joint Inventor: **Alan F. Rodriguez, Jr.**

Residence: 3104 Sneed, Apt. 208
Dallas, Texas 75204
DALLAS COUNTY

Citizenship: USA

Post Office Address: 3104 Sneed, Apt. 208
Dallas, Texas 75204
DALLAS COUNTY

Date: 8 / 1 / 00



Signature

Full Name of


Second Joint Inventor: **Christopher W. Cross**

Residence: 6405 Rock Springs Drive
Arlington, Texas 76001
TARRANT COUNTY

Citizenship: USA

Post Office Address: 6405 Rock Springs Drive
Arlington, Texas 76001
TARRANT COUNTY

Date: 8/8/00



Signature

**Full Name of
Third Joint Inventor:**

Dorwin Shields, Jr.

Residence:

4327 Rosemead Parkway, Apt. 731
Dallas, Texas 75287
COLLIN COUNTY

Citizenship:

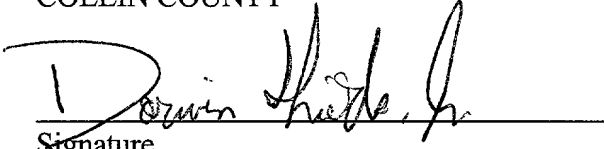
USA

Post Office Address:

4327 Rosemead Parkway, Apt. 731
Dallas, Texas 75287
COLLIN COUNTY

Date:

8-5-2000


Signature

002060 5785960

**Full Name of
Fourth Joint Inventor:**

David T. Meckenstock

Residence:

4918 Big Spring Circle
Missouri City, Texas 77459
FT. BEND COUNTY

Citizenship:

USA

Post Office Address:

4918 Big Spring Circle
Missouri City, Texas 77459
FT. BEND COUNTY

Date: 9/4/00

David T. Meckenstock
Signature

006556845-000700